UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ANGELA ADKINS, on behalf of herself and all others similarly situated, Plaintiff, v. **EVEREST GLOBAL SERVICES, INC.,** Defendant.	Case No. 3:23-cv-00004-MAS-LHG District Judge Michael A. Shipp Magistrate Judge Lois H. Goodman **DEMAND FOR JURY TRIAL**

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff Angela Adkins ("Plaintiff") brings this Second Amended Class Action Complaint, on behalf of herself and all others similarly situated (the "Class Members"), against Defendant Everest Global Services, Inc. ("Everest" or "Defendant") alleging as follows, based upon information and belief, investigation of her counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the targeted cyberattack and data breach ("Data Breach") on Everest's network that resulted in unauthorized access to highly sensitive data.[1] As a result of the Data Breach, Class Members suffered ascertainable losses in the form of, *inter alia*, the benefit of their bargain, loss of privacy, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. Everest provides underwriting and re-insurance services to a global portfolio of

[1] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-13.pdf (last visited Sep. 20, 2024).

insurance companies, including consumer-facing insurance providers. These consumer-facing insurance companies collect PII from Plaintiff and Class Members in the course of offering retail insurance services and provide it to Everest for the purpose of acquiring underwriting or re-insurance services from Everest.

3. Plaintiff and Class Members are individuals whose personally identifiable information ("PII") was acquired, stored, and utilized by Everest in the regular and everyday course of its for-profit business.

4. The specific PII acquired by Everest from Plaintiff's and Class Members' insurance companies and ultimately compromised in the Data Breach includes full names, Social Security numbers, addresses, dates of birth, driver's license numbers, state identification numbers, financial account information, insurance claim numbers, health insurance policy numbers, health information such as medical history, condition, treatment or diagnosis, patient medical numbers, patient account numbers.[2]

5. In or about August of 2022, Everest allowed an unauthorized threat actor access to files containing Plaintiff's and Class Members' PII, which, on information and belief, were stored unencrypted and unredacted on an internet accessible email account.

6. Plaintiff's and Class Members' PII—which was entrusted to Defendant and which Defendant was in an exclusive position to protect—was compromised and unlawfully accessed due to the Data Breach.

7. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's network in a condition vulnerable to cyberattacks and the

[2] https://web.archive.org/web/20231002112957/https://www.doj.nh.gov/consumer/security-breaches/documents/everest-global-services-20221219.pdf (last visited Sep. 20, 2024).

mechanism of the cyberattack (an email phishing attach) and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant. Defendant was thus on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

8. Phishing attacks, like the one apparently experienced by Defendant, are a common but basic attack vector that are designed to entice the recipient into entering company access credentials into fake websites. Due to the frequency of phishing attacks, companies that handle consumer PII and other sensitive information are aware of the need to take measures to prevent them.

9. Defendant could have prevented the unauthorized access to Plaintiff's and Class Members' PII by following basic industry standard measure like ensuring robust passwords, implementing multi-factor authentication, "sandboxing" emails with potential malicious malware, and conducting companywide awareness training for phishing attacks.

10. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network and IT systems that housed Plaintiff's and Class Members' PII and failed to prevent or detect the intrusion or access to PII for more than a week after it began.

11. Plaintiff's PII has already been misused, and Plaintiff's and Class Members' identities are now at imminent risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals.

12. Defendant failed to provide timely, accurate and adequate notice to Plaintiff and Class Members. Plaintiff's and Class Members' knowledge about the PII that Defendant lost control of (by allowing cybercriminals to access it), as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by

Defendant's failure to warn impacted persons for approximately four months after first learning of the data breach.

13. In letters dated December 16, 2022, Defendant notified state Attorneys General and many Class Members about the widespread data breach that had occurred on Defendant's computer network and that Class Members' PII was accessed and acquired by malicious actors (the "Notice Letter" or "Notice Letters").[3]

14. In its required Notice Letter, Defendant "identified suspicious activity associated with its email environment."[4] Defendant became aware of the suspicious activity on August 15, 2022, but did not identify or notify the individuals who had their data stolen. After learning the identities of the affected persons, Defendant still waited months to notify state Attorneys General and Class Members about the widespread Data Breach.

15. Defendant acknowledged its investigation into the Data Breach determined that there was unauthorized access to email accounts between August 8, 2022, and August 16, 2022. Defendant's investigation concluded and it learned what information was present in the accounts and lost to the data thieves on approximately October 10, 2022.

16. Defendant's Notice Letter further admitted that the PII accessed included individuals' names and Social Security numbers.

17. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members'

[3] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-13.pdf (last visited Sep. 20, 2024).
[4] *Id.*

information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. By her Second Amended Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

21. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of her and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown third party. Plaintiff alleges a count of negligence against Defendant and seeks, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services.

THE PARTIES

22. Plaintiff Angela Adkins is a natural person, resident, and a citizen of the State of Ohio. Plaintiff Adkins has no intention of moving to a different state in the immediate future. Plaintiff Adkins is acting on her own behalf and on behalf of others similarly situated. Defendant

obtained Plaintiff Adkins's PII from her insurance company, Farmers Insurance, and it continues to maintain her PII. Because Defendant collects this information for its own profit and is an unexclusive position to protect against the consequences of a foreseeable data breach, Defendant owed and continues to owe her a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Adkins's PII was compromised and disclosed as a result of Defendant's negligent and inadequate data security, which resulted in the Data Breach.

23. Plaintiff would not have allowed Farmers to provide Defendant, or anyone in Defendant's position, her PII had she known that Defendant would fail to implement reasonable and industry standard data security.

24. Plaintiff received a notice letter from Everest dated December 16, 2022, stating that a data security incident occurred at Everest and that her personal information, including her name and Social Security number, was involved in the incident.

25. Defendant Everest Global Services, Inc. is a provider of reinsurance and insurance solutions, operating for decades years through subsidiaries in the United States, Europe, Singapore, Canada, Bermuda and other territories. Everest has is headquartered at 100 Everest Way, Warren, New Jersey 07059.

JURISDICTION AND VENUE

26. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

27. This Court has general personal jurisdiction over Defendant because Defendant maintains principal places of business at 100 Everest Way, Warren, New Jersey 07059 regularly

conducts business in New Jersey, and has sufficient minimum contacts in New Jersey. Defendant intentionally availed itself of this jurisdiction by marketing and selling its services from New Jersey to many businesses nationwide.

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANT'S BUSINESSES

29. Defendant Everest Global Services, Inc. is a provider of reinsurance and insurance, operating for decades years through subsidiaries in the United States, Europe, Singapore, Canada, Bermuda, and other territories.

30. Defendant provides reinsurance and other services to many insurance companies, including consumer facing insurance companies that offer retail insurance services like Farmers Insurance and its subsidiaries.[5]

31. On information and belief, in the ordinary course of providing insurance and reinsurance services, Defendant maintains the PII of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Photo identification;

[5] See https://www.insurance.ca.gov/0250-insurers/0300-insurers/0400-reports-examination/upload/Farmers-Insurance-Group-Consolidated-Exam-Report-Final-as-of-12-2021.pdf (last visited Sep. 20, 2024).

- Medical information;
- Employment information, and;
- Other information that Defendant may deem necessary to provide its services.

32. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its insurance company clients' customers, and because it derives a pecuniary benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from the foreseeable risk of unauthorized disclosure.

33. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and expect that any business lawfully in possession of their PII while also take reasonable measures to safeguard its confidentiality.

34. Plaintiff and the Class Members relied on Defendant, and anyone in Defendant's position, to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

THE CYBERATTACK

35. On or around August 15, 2022, Defendant became aware of suspicious activity in its network environment, specifically related to its email environment.

36. Defendant investigated the suspicious activity with the assistance of a third-party computer forensic expert.

37. Through its investigation, Defendant determined that certain email accounts stored on its network and servers were subject to a cyber-attack that impacted its network where information on its network was accessed and acquired without authorization.

38. The investigation determined that email accounts containing unencrypted PII related to certain consumers (including Plaintiff) were accessed and taken by an unauthorized user between August 8, 2022, and August 16, 2022.

39. In a December 16, 2022, letter to the New Hampshire Attorney General, Defendant stated that:

> On August 15, 2022, Everest identified suspicious activity associated with its email environment. Everest immediately implemented its incident response protocols, took steps to secure the email environment, and engaged external cybersecurity experts to conduct a forensic investigation. The investigation found that there was unauthorized access to five email accounts between August 8, 2022 and August 16, 2022. A third-party vendor was engaged to review the contents of these email accounts to identify and extract any personally identifiable information that may have been affected. Everest determined that personally identifiable information was present within the accounts on approximately October 10, 2022.
> …
> Impacted information may include names and some combination of the following: addresses, Social Security numbers, dates of birth, driver's license numbers, state identification numbers, financial account information, insurance claim numbers, health insurance policy numbers, health information such as medical history, condition, treatment or diagnosis, patient medical numbers, patient account numbers.
> …
> Since this event, Everest has, among other actions, reset passwords for email accounts, reinforced multi-factor authentication measures (which were previously enabled on all email accounts), and increased the frequency of mandatory company-wide training and awareness of increasing cyber risks. Additionally, impacted individuals were offered 12 months of credit monitoring and identity protection services through IDX.[6]

40. Notice Letters that Defendant sent to Plaintiff and Class Members recommended that they "vigilantly monitor [their] financial statements and credit reports and immediately report any suspicious activity."[7] The Notice Letters further provided the following "Recommended Steps

[6] https://web.archive.org/web/20231002112957/https://www.doj.nh.gov/consumer/security-breaches/documents/everest-global-services-20221219.pdf (last visited Sep. 20, 2024).
[7] https://web.archive.org/web/20231002112957/https://www.doj.nh.gov/consumer/security-breaches/documents/everest-global-services-20221219.pdf (last visited Sep. 20, 2024).

to Help Protect Your Information":

> We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.
> …
>
> Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:
> …
>
> Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.[8]

41. Upon information and belief, Plaintiff's and Class Members' PII was exfiltrated and stolen in the attack. The five, accessed email accounts contained PII that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

42. It is likely the Data Breach was targeted at Defendant due to its status as a company in the insurance and reinsurance business that collects, creates, and maintains vast amounts of

[8] *See, e.g., id.*

consumer PII that it receives from its consumer-facing insurance company clients.

43. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

44. Defendant admitted that the stolen information may have included full names and Social Security Numbers.

45. While Defendant stated in the Notice Letter that the unusual activity occurred and was discovered on August 15, 2022, and was accessed for over a full week, Defendant failed to notify the specific persons or entities whose PII was acquired and exfiltrated until December 16, 2022– over four months later.

46. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiff's PII was stolen in the Data Breach. Plaintiff further believes her PII was subsequently misused by the cybercriminal and/or sold on the dark web, as she has experienced unauthorized access to her financial accounts and been the target of phishing attempts following the Data Breach.

47. As Defendant acknowledged in its Notice Letters, Defendant takes "the security of information is very important to us."[9]

48. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

49. In response to the Data Breach, Defendant admits they worked with "computer forensic experts" to determine the nature and scope of the incident and purports to have taken steps to secure the systems. Defendant admits additional security was required, but there is no indication

[9] *Id.*

whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

50. Because of the Data Breach, data thieves were able to gain access to Defendant's IT systems for 8 days (between August 8, 2022, and August 16, 2021) and were able to compromise, access, and acquire the protected PII of Plaintiff and Class Members.

51. As a company that collects and uses consumer PII for its own for-profit business, Defendant had obligations created by contract, industry standards, common law, and its own promises and representations regarding their duty to keep their PII confidential and to protect it from unauthorized access and disclosure.

52. As a partner to and recipient of information from their insurance companies Plaintiff and the Class Members reasonably relied (directly or indirectly) on this sophisticated insurance institution to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

53. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Defendant negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

54. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance industry and other industries holding significant amounts of PII preceding the date of the breach.

55. Two years ago, Defendant published a blog post on its website admitting that data

breaches are prevalent, and that data protection is important[10], yet still failed to adequately secure its systems and network to prevent the Data Breach.

56. Moreover, in light of recent high profile data breaches at other insurance partner and provider companies, e.g., Wilton Reassurance Company (1.4 million records, June 2023), Defendant knew or should have known that the consumer PII they maintained would be targeted by cybercriminals.

57. In 2021, the year preceding the Data Breach, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

58. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Comply with its own Policies

59. In its Notice Letter to Plaintiff and Class Members, Defendant acknowledged the importance of data security and the privacy of individuals' PII.

60. Further, Defendant acknowledges its own obligation to safeguard consumer PII and

[10] "Increasingly costly data breaches in recent years have shown the importance of data protection and privacy in the age of the data economy. While organizations have accelerated their pace in adapting to the increased levels of security and data sharing, much still needs to be done." Self-aware Data – Securing Data across its Life Cycle, Dec. 16, 2022: https://www.everestgrp.com/tag/data-breach/ (last visited Sep. 20, 2024).

[11] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/) (last visited Sep. 20, 2024).

[12] *Id.*

represents on its public website that "Everest is committed to conducting business in a compliant manner while taking steps to safeguard personal data we receive, collect, transfer, and store in the course of doing business."[13]

61. Defendant also maintains a Privacy Notice on its website, "on behalf of the Everest companies, subsidiaries, and affiliates" applying to "current and former customers, business partners, employees, job applicants, and others who reside in the United States."[14] This Privacy Notice, therefore, purports to set forth Defendant's privacy policy where Plaintiff and Class Members are concerned, regardless of the direct or indirect nature of their relationship with Defendant.

62. This Privacy Notice states:

> We maintain physical, electronic and administrative safeguards designed to help protect personal information. We secure our databases with various physical, technical and procedural measures, and we restrict access to your information by unauthorized persons.
>
> We also train all employees on their responsibility to safeguard customer data and provide them with appropriate guidelines for adhering to our company's business ethics, standards, and confidentiality policies.
>
> Encryption, and other methods are used to protect sensitive information. The method of protection is based on the sensitivity of the data that is shared with customers and other third parties under contract to do business with Everest.
>
> We take particular care when working with third parties, only sharing personal data with affiliates, business partners, third-party service providers, or vendors when we have a legitimate business purpose for doing so. We ensure contractual requirements, including confidentiality clauses, are in place to ensure Everest's data protection principals are adhered to.[15]

63. That Defendant dedicates considerable language on its website to the importance

[13] https://www.everestglobal.com/us-en/about-us/privacy/privacy-security-and-trust
[14] https://www.everestglobal.com/us-en/about-us/privacy/privacy-security-and-trust/privacy-notices-and-policies/us-privacy-notice
[15] *Id.*

of data security and data privacy, clearly suggests that Defendant is aware of that damage that can be done if PII is mistreated or misused. These statements concerning privacy are evidence that Defendant acknowledges its statutory and common law duties to, in its own words, "safeguard personal data we retrieve, collect, transfer, and store in the course of doing business."[16]

64. Most importantly however, once Defendant acquired Plaintiff's and Class Members' PII, Defendant alone was in an exclusive position to safeguard it from unauthorized access as Plaintiff had no knowledge of Defendant's data security practices and no ability to influence those practices.

Defendant Fail to Comply with FTC Guidelines

65. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

[16] https://www.everestglobal.com/us-en/about-us/privacy/privacy-security-and-trust
[17] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sep. 20, 2024).

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. These FTC enforcement actions include actions against insurance providers and partners like Defendant.

70. Defendant failed to properly implement basic data security practices.

71. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

72. Defendant was at all times fully aware of its obligation to protect the PII of consumers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[18] *Id.*

Defendant Failed to Comply with Industry Standards

73. Several best practices have been identified by experts studying cyber security that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

74. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

75. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

DEFENDANT'S BREACH

77. Defendant breached its obligations and duties to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard

its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;

e. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. Failing to encrypt consumer PII when in transit and at rest, allowing its employees to transmit and receive unencrypted PII via email, and allowing employees to hold emails containing unencrypted PII in their email accounts;

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

k. Failing to train all members of its workforces effectively on the policies and procedures regarding PII;

l. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

n. Failing to adhere to industry standards for cybersecurity as discussed above; and,

o. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

78. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted PII.

79. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

80. Cyberattacks and data breaches at insurance companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

81. The United States Government Accountability Office released a report in 2007

regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[19]

82. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

83. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit

[19] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 20, 2024).

reports.[20]

84. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

85. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

86. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[21]

87. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

88. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

89. According to the U.S. Government Accountability Office, which conducted a study

[20] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Sep. 20, 2024).

[21] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

90. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

91. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

92. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

93. PII can sell for as much as $363 per record according to the Infosec Institute.[23] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

94. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[24] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for

---

[22] GAO Report, at p. 29.

[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 20, 2024).

[24] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sep. 20, 2024).

unemployment benefits, or apply for a job using a false identity.[25] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

95. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

96. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

97. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[27]

98. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial

[25] *Id* at 4.
[26] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sep. 20, 2024).
[27] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sep. 20, 2024).

information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[28]

99. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[29]

100. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[30] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[31]

101. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[32]

---

[28] *See* N.C. Gen. Stat. § 132-1.10(1).

[29] *See* https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers

[30] *See* https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/

[31] *See* https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/

[32] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone

102. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

103. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

104. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff and the other Class Members.

105. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

106. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[33]

---

with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

[33] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

107. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[34,35]

108. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[36]

109. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

110. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

111. Because of the value of its collected and stored data, the insurance industry has experienced disproportionally higher numbers of data theft events than other industries.

112. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly

[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[35] https://datacoup.com/
[36] https://digi.me/what-is-digime/

prepare for that risk.

Plaintiff's and Class Members' Damages

113. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

114. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

115. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

116. Plaintiff and Class Members' full names and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer network.

117. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

118. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

119. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of

harm from fraud and identity theft.

121. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

122. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

123. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members. Plaintiff has already experienced various phishing attempts by telephone and through electronic mail.

124. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

125. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

126. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer system and Plaintiff's and Class Members' PII. Thus, the Plaintiff and the Class Members did not get what they paid for and agreed to.

127. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

128. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

129. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

130. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

131. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Adkins' Experience

132. Plaintiff Adkins is a natural person and is, and has been at all times relevant herein, a resident of the state of Ohio.

133. Plaintiff receives insurance services through Farmers Insurance, a company that uses or has used Defendant's services. Plaintiff has been a customer of Farmers Insurance since it acquired MetLife Inc. in 2021.

134. On information and belief, Farmers Insurance is a client of Everest and provided Defendant with Plaintiff's PII in course of receiving underwriting or re-insurance solutions from Defendant.

135. Plaintiff has paid for the insurances services she has received from Farmers Insurance and Farmers in turn pays Everest for its services, indirectly conferring a monetary benefit on Defendant.

136. In February 2023, Plaintiff Adkins discovered that an unauthorized third party attempted to access her Fifth Third Bank joint-checking account and a payment debit card directly linked to that account. As a result of the fraud, the payment card associated with the joint-checking account was closed by Plaintiff's bank without notice.

137. Plaintiff first became aware of the problem with her joint account that she shares

with her husband when the associated debit card was declined in late February 2023 as Plaintiff's husband attempted to purchase gasoline for their vehicle that is titled in Plaintiff's name and that Plaintiff and her husband share.

138. Plaintiff's spouse was forced to drive Plaintiff's vehicle to a Fifth Third bank branch location so that he could access the account, withdraw cash, and have a new payment card issued. The new payment card took approximately one week to arrive. Moreover, the trip to the bank in Plaintiff's vehicle caused the consumption of gasoline and wear and tear on the vehicle belonging to Plaintiff.

139. Several other online automatic payments that were set-up to withdraw from Plaintiff's joint-checking account, including her family's YouTube TV, Netflix, Apple Pay, and Apple Music subscriptions were subsequently declined, and the services halted. Plaintiff lost access to these accounts until a new payment method was established.

140. Plaintiff Adkins is very careful with her Private Information. She stores any documents containing PII a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. When Plaintiff does entrust a third-party with her PII, it is only because she understands the PII will be safeguarded from reasonably foreseeable threats.

141. Plaintiff Adkins provided PII, including her name and Social Security number, to Farmers Insurance, one of Defendant's clients, who in turn provided it to Defendant, in the course of providing her retail insurance services. On information and belief, Farmers Insurance provided Everest with Plaintiff's PII as a condition of receiving underwriting or re-insurance services from Everest.

142. Plaintiff Adkins first learned of the Data Breach after receiving a data breach

notification letter dated December 16, 2022, from Everest, notifying her that Defendant suffered a data breach four months prior and that her PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

143. The data breach notification letter indicated that the PII involved in the Data Breach included Plaintiff Adkins's full name and Social Security number.

144. As a result of the Data Breach, Plaintiff Adkins made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

145. Plaintiff Adkins was forced to spend multiple hours attempting to resolve issues related to the Data Breach and the resulting fraud that she suffered. Plaintiff Adkins will continue to spend valuable time for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

146. Plaintiff Adkins suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Adkins; (b) loss of privacy; (c) the theft of her PII; and (d) actual injury arising from identity theft and fraud.

147. Plaintiff Adkins has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Adkins is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

148. As a result of the Data Breach, Plaintiff Adkins anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Adkins will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

149. Plaintiff Adkins has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up on Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

150. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

151. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All residents of the United States identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

152. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

153. Plaintiff reserves the right to amend or modify the Class or Subclass definitions as this case progresses.

154. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, upon information and belief, the Class consists of thousands of

individuals whose sensitive data was compromised in the Data Breach, since Defendants reported that 403 Texas residents alone were impacted by the Data Breach.[37]

155. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages

[37] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited April 2, 2023).

as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

l. Whether Plaintiff and Class Members are entitled to damages and/or injunctive relief.

156. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

157. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

158. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

159. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

160. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

161. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented

the Data Breach.

162. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

163. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Second Amended Complaint as if fully set forth herein.

164. Plaintiff and Class Members are individuals who, either directly or indirectly, were required to confer their PII on Defendant in the ordinary course of receiving insurance or reinsurance services through Defendant's business clients.

165. Plaintiff and Class Members provided their PII to their insurance companies who in turn provided the PII to Defendant as a condition of receiving Defendant's underwriting or reinsurance services.

166. By collecting and storing this data in its computer system and network, and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

167. Defendant owed a duty of care to Plaintiff and Class Members to provide data

security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

168. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members by virtue of the fact that Defendant was in an exclusive position to protect Plaintiff's and Class Members' PII from a foreseeable threat and because Plaintiff and Class Members had no ability to influence Defendant's data security posture and were entirely dependent on Defendant to implement reasonable and expected data security measures. Once Defendant acquired the PII, Defendant was in an exclusive and superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

169. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

170. Defendant explicitly acknowledged these duties and the importance of carrying them out in its statements on privacy found on its public website.[38]

171. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

172. To the extent Ohio law applies, Defendant had a duty to Plaintiff and other Ohio Class Members as evidenced by Ohio Revised Code 1354.01, *et seq.*

173. Defendant's duty to use reasonable care in protecting confidential data arose not

[38] *See* https://www.everestglobal.com/us-en/about-us/privacy/privacy-security-and-trust

only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

174. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to implement multi-factor authentication on all accounts with access to sensitive PII;

c. Failing to implement a phishing awareness training program;

d. Failing to encrypt consumer PII when in transit and at rest, allowing its employees to transmit and receive unencrypted PII via email, and allowing employees to hold emails containing unencrypted PII in their email accounts;

e. Failing to adequately monitor the security of its networks and systems;

f. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

g. Failing to have in place mitigation policies and procedures;

h. Allowing unauthorized access to Class Members' PII;

i. Failing to detect in a timely manner that Class Members' PII had been compromised; and

j. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and

other damages.

175. Due to the nature of the relationship with Defendant, Plaintiff and Class Members had no ability to protect their PII that was, or remains, in Defendant's possession.

176. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

177. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

178. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

179. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII.

180. The duties owed to Plaintiff and Class Members are separate from and untethered to any contractual obligations.

181. The risk that unauthorized persons would attempt to gain access to the PII and

misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by phishing attempts or otherwise.

182. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the unredacted and unencrypted PII of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

183. Defendant breached its duties by failing to exercise reasonable care in handling and securing the PII of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

184. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

185. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, loss or privacy from the authorized access and exfiltration of their PII; and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

e) For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, as allowable by law;

f) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

g) Pre- and post-judgment interest on any amounts awarded; and,

h) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demand a trial by jury of any and all issues in this action so triable as of right.

Dated: September 20, 2024

Respectfully Submitted,

Vicki J. Maniatis
Vicki J. Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite
500 Garden City, New York
11530 Tel.:(865) 412-2700
vmaniatis@milberg.com

Gary M. Klinger (*Admitted Pro Hac Vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Terence R. Coates (*Admitted Pro Hac Vice*)
Justin C. Walker (*Admitted Pro Hac Vice*)
Jonathan T. Deters*
Markovits, Stock & DeMarco, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
jdeters@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

* *Pro Hac Vice* Forthcoming

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the above document was served upon all counsel of record via ECF electronic filing on September 20, 2024.

/s/ Vicki J. Maniatis
Vicki J. Maniatis